Zienswijze van de CTIVD

Op het wetsvoorstel Wiv 20..

november 2016

Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten

Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten

ZIENSWIJZE VAN DE CTIVD

Op het wetsvoorstel Wiv 20..

Op 28 oktober 2016 stuurde het kabinet het voorstel voor een nieuwe Wet op de inlichtingen- en veiligheidsdiensten naar de Tweede Kamer. De Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD) geeft hierbij haar zienswijze op dit wetsvoorstel. Zij beschikt als onafhankelijk toezichthouder, die rechtstreeks toegang heeft tot de AIVD en de MIVD, over een expertise en deskundigheid die haar goed in staat stelt de inhoud van het wetsvoorstel en de toepassing daarvan in de praktijk op waarde te schatten. Deze zienswijze beoogt handvatten te bieden ten behoeve van de parlementaire behandeling van het wetsvoorstel.

Evenwicht bereikt?

Vanuit haar ervaring en kennis van de praktijk, wil de CTIVD inzicht geven in het evenwicht dat in de nieuwe wet op de inlichtingen- en veiligheidsdiensten (Wiv 20..) haars inziens moet worden bereikt. Een evenwicht tussen enerzijds bevoegdheden die noodzakelijk zijn om bedreigingen van de nationale veiligheid tijdig te kunnen onderkennen en anderzijds waarborgen die effectieve bescherming bieden tegen ongeoorloofde inbreuken op onze grondrechten, waaronder de privacy. Dit evenwicht is naar het oordeel van de CTIVD in het wetsvoorstel Wiv 20.. niet bereikt. De aanbevelingen opgenomen in deze zienswijze zijn erop gericht de ontbrekende essentiële waarborgen te duiden. Wettelijke waarborgen die nu én in de toekomst privacybescherming garanderen, effectief toezicht mogelijk maken en tegelijk de AIVD en de MIVD geen onnodige beperkingen opleggen in de uitvoering van de wettelijke taak die aan hen is opgedragen.

Uitbreiding en modernisering bevoegdheden

Het beeld dat de CTIVD heeft van de reikwijdte van de bestaande bevoegdheden van de AIVD en de MIVD, gerelateerd aan de vraag of deze diensten daarmee nog altijd in staat moeten worden geacht de hedendaagse en toekomstige dreigingen voor de nationale veiligheid in de praktijk tijdig te pareren, bevestigt de noodzaak van de voorgestelde uitbreiding daarvan. Daarbij spelen niet alleen veranderingen in de aard en omvang van deze dreigingen een rol, gemeten naar ernst en waarschijnlijkheid, maar evengoed de technologische en maatschappelijke ontwikkelingen van de afgelopen jaren. Ontwikkelingen die zien op het in rap tempo ontstaan van een gedigitaliseerde samenleving met steeds weer geheel nieuwe communicatiemiddelen en –methoden, die hebben geleid en verder zullen leiden tot een exponentiële groei van communicatie en dataverkeer. Een groei met navenant grote hoeveelheden gegevens die wereldwijd worden getransporteerd en opgeslagen. Gegevensverzamelingen, die voor diensten als de AIVD en de MIVD bepalend kunnen zijn voor een goede taakuitvoering.

Meer dan nu al het geval is, betekent uitbreiding en modernisering van de bevoegdheden dat de diensten de beschikking (zullen) krijgen over steeds grotere hoeveelheden gegevens. De sterke toename van gegevensuitwisseling in internationaal verband draagt hier evenzeer aan bij. De herkomst en betrouwbaarheid van al deze gegevens verdient voortdurende aandacht. Noodzakelijkerwijs worden ook steeds meer technieken ontwikkeld en ingezet die geautomatiseerde verwerking van deze gegevens, van verzamelen en analyseren tot vernietigen, mogelijk maakt. Niet alleen de hoeveelheid gegevens, maar ook de complexiteit van de gegevensverwerking is daarmee toegenomen en zal in de toekomst blijven groeien.

Versterking van waarborgen en toezicht

De waarborgen voor de bescherming van de privacy en andere grondrechten dienen één op één mee te gaan in bovenstaande ontwikkelingen. Waar sprake is van het in grotere hoeveelheden verzamelen, ontvangen en verwerken van gegevens, is immers ook sprake van grotere hoeveelheden gegevens van personen en organisaties die géén doelwit van de diensten zijn. Dit leidt tot een groter risico op ongeoorloofde inbreuken op de privacy. Complexe en geautomatiseerde vormen van gegevensverwerking brengen evenzeer risico's met zich mee die aanvullende waarborgen vereisen tegen ongeoorloofd gebruik daarvan. Het gaat hier onder meer om waarborgen voor de kwaliteit van systemen die op basis van bepaalde kenmerken gegevensverzamelingen geautomatiseerd toegankelijk maken of van technieken die op basis van gedragsmodellen en profielen gegevens uitlichten.

In het wetsvoorstel wordt de nadruk sterk gelegd op klassieke waarborgen, zoals voorafgaande toestemmingsverlening (minister) en toetsing (toetsingscommissie inzet bevoegdheden (TIB)) voor de inzet van de bevoegdheden. Hoewel deze waarborgen aanzienlijk zijn versterkt ten opzichte van de huidige wettelijke regeling zijn deze alléén, niet meer toereikend. Juist voor het verzamelen en verder verwerken van grote hoeveelheden gegevens (bulk), met name ten behoeve van het vaststellen van nog ongekende dreigingen, heeft het beperkte betekenis een motivering gekoppeld aan toestemming en onafhankelijke toetsing aan de voorkant van het proces te eisen. Men weet immers vaak op voorhand nog niet naar wie en wat men precies zoekt. Een dergelijk systeem van waarborgen vooraf krijgt vooral inhoud bij de gerichte inzet van bevoegdheden bij een gekende dreiging, waarbij een persoon of organisatie al in beeld is.

Klassieke waarborgen alléén zijn niet meer toereikend

Juist voor de verwerking van steeds grotere hoeveelheden gegevens zijn aanvullende, toekomstvaste waarborgen noodzakelijk. Deze waarborgen moeten zien op die fase van het gegevensverwerkingsproces waar de (privacy)inbreuk daadwerkelijk plaatsvindt, te weten tijdens de geautomatiseerde bewerkings-, analyse- en gebruiksfase. Die waarborgen moeten adequaat en toetsbaar zijn. Een wettelijke zorgplicht voor geautomatiseerde gegevensverwerking, die nu in het wetsvoorstel ontbreekt, is in dat kader essentieel. Deze zorgplicht moet inhouden dat de diensten door middel van een bij wet vastgelegd instrumentarium verantwoording afleggen over de kwaliteit van de geautomatiseerde gegevensverwerkingsprocessen en dat hierop effectief toezicht kan worden gehouden. Daarbij kan overigens niet voorbij worden gegaan aan de operationele realiteit waarmee de AIVD en de MIVD dagelijks te maken hebben. Dit laatste houdt in dat er oog moet zijn voor de omvang van de administratieve last die de diensten wordt opgelegd.

Versterking van het toezicht geldt bij de hiervoor genoemde ontwikkelingen als een harde randvoorwaarde. Effectief toezicht vereist toezicht dat in staat is zich te laten gelden juist daar waar de inbreuk op grondrechten zich het sterkst doet voelen. Het toezicht zal zich dan ook moeten kunnen richten op technologische en systeemtechnische toepassingen en de effecten hiervan op de privacy en andere grondrechten. Met alleen de huidige voorstellen, waarbij de nadruk ligt op toestemmingsverlening en toetsing vooraf, wordt deze effectiviteit niet bereikt.

Aanvulling en aanscherping essentieel

De CTIVD bespreekt in deze zienswijze vijf thema's die van betekenis zijn voor het bereiken van een passend evenwicht in de nieuwe wet tussen enerzijds bevoegdheden en anderzijds waarborgen tegen ongeoorloofd gebruik daarvan. Hieronder wordt kort uiteengezet op welke onderdelen aanvulling of aanscherping naar het oordeel van de CTIVD essentieel is. Daarbij is het van belang op te merken dat het opvolgen van de aanbevelingen van de CTIVD ook gepaard dient te gaan met voldoende middelen voor de diensten om aanvullende waarborgen daadwerkelijk in te richten en voor de toezichthouder(s) om op de werking daarvan toe te zien. Zonder de toekenning hiervan zullen waarborgen geen inhoud krijgen en zal toezicht niet effectief kunnen zijn.

Effectief toezicht vereist toezicht dat in staat is zich te laten gelden juist daar waar de inbreuk op grondrechten zich het sterkst doet voelen

Toezicht

Het toezicht mist in het wetsvoorstel voldoende effectiviteit waar het gaat om toezicht op geautomatiseerde gegevensverwerking. Ook strekt het tot aanbeveling de reikwijdte van het toezicht ten opzichte van de toetsing door de TIB te verduidelijken, teneinde een toezichtshiaat te voorkomen. Verder voorziet het wetsvoorstel niet in waarborgen ten behoeve van uniforme en consistente rechtstoepassing, de rechtseenheid. Het in het wetsvoorstel beschreven systeem van voorafgaande toestemming (minister) en toetsing (TIB of rechter) en van toezicht en klachtbehandeling achteraf (CTIVD), is gelaagd en complex. Alle genoemde spelers zullen zich met dezelfde rechtsvragen bezig gaan houden. Het is van belang dat de uniforme en consistente rechtstoepassing in de nieuwe wet wordt geadresseerd, door de TIB en de CTIVD de gezamenlijke taak te geven de rechtseenheid te bevorderen. **(Bijlage I, paragraaf 1)**

Interceptie

Het voorgestelde interceptiestelsel, dat simpelweg complex is, bevat nog geen adequaat systeem van wettelijke waarborgen. Weliswaar is in het wetsvoorstel sprake van een aanzienlijke versterking van voorafgaande toestemming en toetsing van de inzet van de bulkinterceptiebevoegdheden, maar deze gekozen systematiek adresseert slechts in beperkte mate de risico's voor de bescherming van onze grondrechten, die bulkinterceptie met zich meebrengt. Deze risico's kunnen worden beperkt door te zorgen voor een "verantwoorde databeperking". De kern hiervan is dat gegevens altijd zo gericht mogelijk dienen te worden verworven en dat verworven gegevens zo spoedig mogelijk moeten worden

gereduceerd tot die gegevens die de AIVD en de MIVD daadwerkelijk nodig hebben om hun taken goed uit te voeren. Niet meer en ook niet minder.

Het voorgestelde interceptiestelsel, dat simpelweg complex is, bevat nog geen adequaat systeem van wettelijke waarborgen

Hoewel het wetsvoorstel en de gegeven toelichting weliswaar beogen invulling te geven aan deze "verantwoorde databeperking", ontbreken de waarborgen daartoe of missen deze een duidelijke bepaling in de wet. Het is van essentieel belang dat "verantwoorde databeperking" nadere invulling krijgt. Enerzijds door het vereiste in de wet op te nemen dat de inzet van bevoegdheden "zo gericht mogelijk" moet zijn. Anderzijds door de doelgerichtheid bij de verwerking van gegevens te verankeren in concrete wettelijke plichten die ervoor zorgen dat de interceptie en verdere verwerking daadwerkelijk onderzoeksopdrachtgericht gebeurt, de opslag van gegevens daarmee wordt beperkt, vernietiging van gegevens tijdig plaatsvindt en dat op dit alles effectief toezicht kan worden gehouden. **(Bijlage I, paragraaf 2)**

Geautomatiseerde gegevensverwerking

Aan het gebruik van geautomatiseerde verwerkingsprocessen kleven risico's. Zo bestaat het gevaar dat bij complexe en grootschalige gegevensverwerkingsprocessen het voor de diensten zelf en de toezichthouder steeds minder transparant of navolgbaar is welke gegevens op welke manier worden verwerkt. Complicerende factor daarbij is dat juist deze geautomatiseerde verwerkingsprocessen ook belangrijke waarborgfuncties kunnen vervullen, bijvoorbeeld het geautomatiseerd vernietigen van gegevens als de bewaartermijn is verstreken of het stoppen met het verzamelen van gegevens als de toestemmingsperiode daarvoor is afgelopen. Ook wordt in toenemende mate gebruik gemaakt van geautomatiseerde analyseprocessen, zoals Big Data analyse. Het is van evident belang dat de diensten moeten kunnen garanderen dat geautomatiseerde gegevensverwerkingsprocessen doen wat daarvan wordt verwacht en dat de toezichthouder dit moet kunnen toetsen. Met de in het wetsvoorstel aangegeven instrumenten is goed toezicht hierop niet mogelijk.

Met de in het wetsvoorstel aangegeven instrumenten is goed toezicht op geautomatiseerde gegevensverwerking niet mogelijk

In de wet dient daarom voor geautomatiseerde gegevensverwerking een zorgplicht voor de diensten opgenomen te worden. Deze zorgplicht strekt zich onder meer uit tot de kwaliteit van de gegevensvergaring, van de gebruikte gegevens(bestanden), van de toe te passen algoritmes en modellen en tot de kwaliteit van de resultaten van deze processen. Hierover moeten de diensten verantwoording afleggen (compliance). De toezichthouder is daarmee in staat effectief te toetsen of geautomatiseerde gegevensverwerking rechtmatig plaatsvindt en hierover te rapporteren aan het Parlement. Daarnaast is het noodzakelijk dat meer vormen van geautomatiseerde data-analyse als bijzondere bevoegdheid worden aangemerkt met de daarbij passende waarborgen. **(Bijlage I, paragraaf 3)**

Hacken
Met betrekking tot de bevoegdheid tot het hacken via derden moeten in het wetsvoorstel aanvullende waarborgen worden opgenomen, gericht op beperking van het derdenbegrip zelf (er moet sprake zijn van een directe technische relatie), op de inzet van deze bevoegdheid (slechts wanneer dat onvermijdelijk is) en op de vernietiging (terstond) van verzamelde gegevens die geen betrekking hebben op het eigenlijke doelwit. **(Bijlage I, paragraaf 4)**

Samenwerking buitenlandse diensten
De rechtsbescherming die met de toets op basis van de samenwerkingscriteria wordt beoogd, verdient een aanmerkelijke versterking. Zo is het van essentieel belang dat het algemene kader voor samenwerkingsrelaties geldt voor alle vormen van gegevensverstrekking en dat een regeling wordt getroffen voor uitzonderingssituaties die is voorzien van adequate waarborgen. Ook dienen in de wet aanvullende criteria voor samenwerking te worden opgenomen en dient de overgangsbepaling die de toepassing van de criteria voor samenwerking met twee jaar uitstelt te worden geschrapt. Verder is het van belang dat de verantwoordelijkheid van de betrokken minister voor de samenwerking met buitenlandse diensten nadrukkelijk invulling krijgt bij het vaststellen van het kader voor de samenwerkingsrelatie en bij samenwerking die afwijkt van dat kader. **(Bijlage I, paragraaf 5)**

De rechtsbescherming bij de samenwerking met buitenlandse diensten verdient een aanmerkelijke versterking

Ten slotte

De CTIVD concretiseert deze aanbevelingen in **bijlage I**, waarin de nu nog in het wetsvoorstel ontbrekende, essentiële waarborgen worden besproken. Per thema wordt uiteengezet wat de kern is van de overwegingen van de CTIVD en worden concrete handvatten geboden voor het versterken van waarborgen en effectief toezicht. In **bijlage II** zijn voorstellen tot kwaliteitsverbeteringen opgenomen die een meer wetstechnisch of op zichzelf staand karakter hebben. In elk van de bijlagen worden per onderdeel aanknopingspunten voor verduidelijking of aanpassing van de voorgestelde wettelijke bepalingen gegeven.

Anna van Saksenlaan 50 | 2593 HT Den Haag
T 070 315 58 20 | **F** 070 381 71 68
E info@ctivd.nl | www.ctivd.nl